(12) UK Patent Application (19) GB (11) 2 237 670 (13) A

(43) Date of A publication 08.05.1991

(21) Application No 9023551.6

(22) Date of filing 30.10.1990

(30) Priority data
(31) 8924847 (32) 03.11.1989 (33) GB

(51) INT CL⁵
G07F 7/10

(52) UK CL (Edition K)
G4H HTG H1A H13D H14A H14D

(56) Documents cited
GB 2112190 A WO 80/02080 A1

(58) Field of search
UK CL (Edition K) G4H HTG
INT CL⁵ G06K, G07F

(71) Applicants
De La Rue Systems Limited

(Incorporated in the United Kingdom)

3/5 Burlington Gardens, London, W1A 1DL, United Kingdom

Midland Bank Plc

(Incorporated in the United Kingdom)

27/32 Poultry, London, EC2P 2BX, United Kingdom

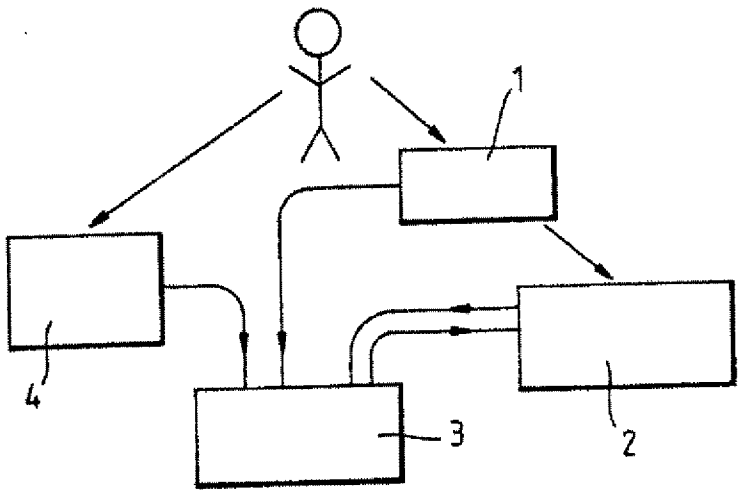
(72) Inventors
Fergus Ion Duncan
William Carter

(74) Agent and/or Address for Service
Gill Jennings & Every
53-64 Chancery Lane, London, WC2A 1HN, United Kingdom

(54) Reciprocal transfer system

(57) A reciprocal transfer system for transfer involving a user and supplier (e.g. retailer) comprises a biometric feature analyser (4) which obtains at least one feature from the user and verifies it to provide a resulting parameter. This parameter is combined with other parameters which may be unrelated to the identification of the user to produce a final risk assessment parameter. Control means (3) indicate to the supplier whether or not the transaction should proceed in accordance with the final risk assessment parameter.

Fig. 1.



GB 2 237 670

Fig.1.

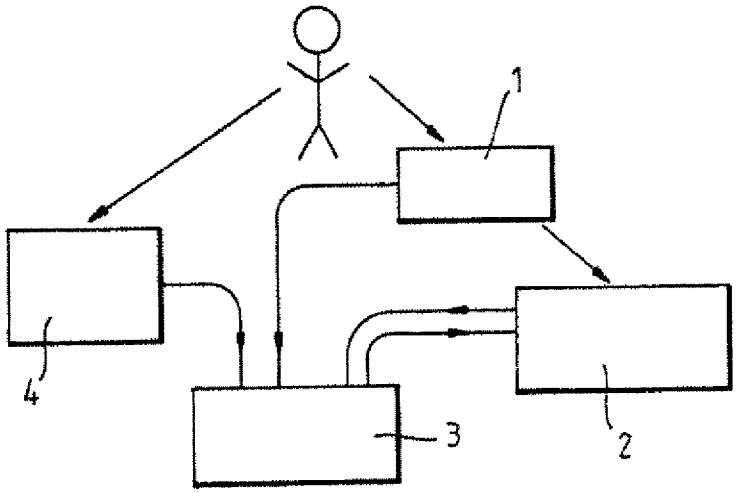
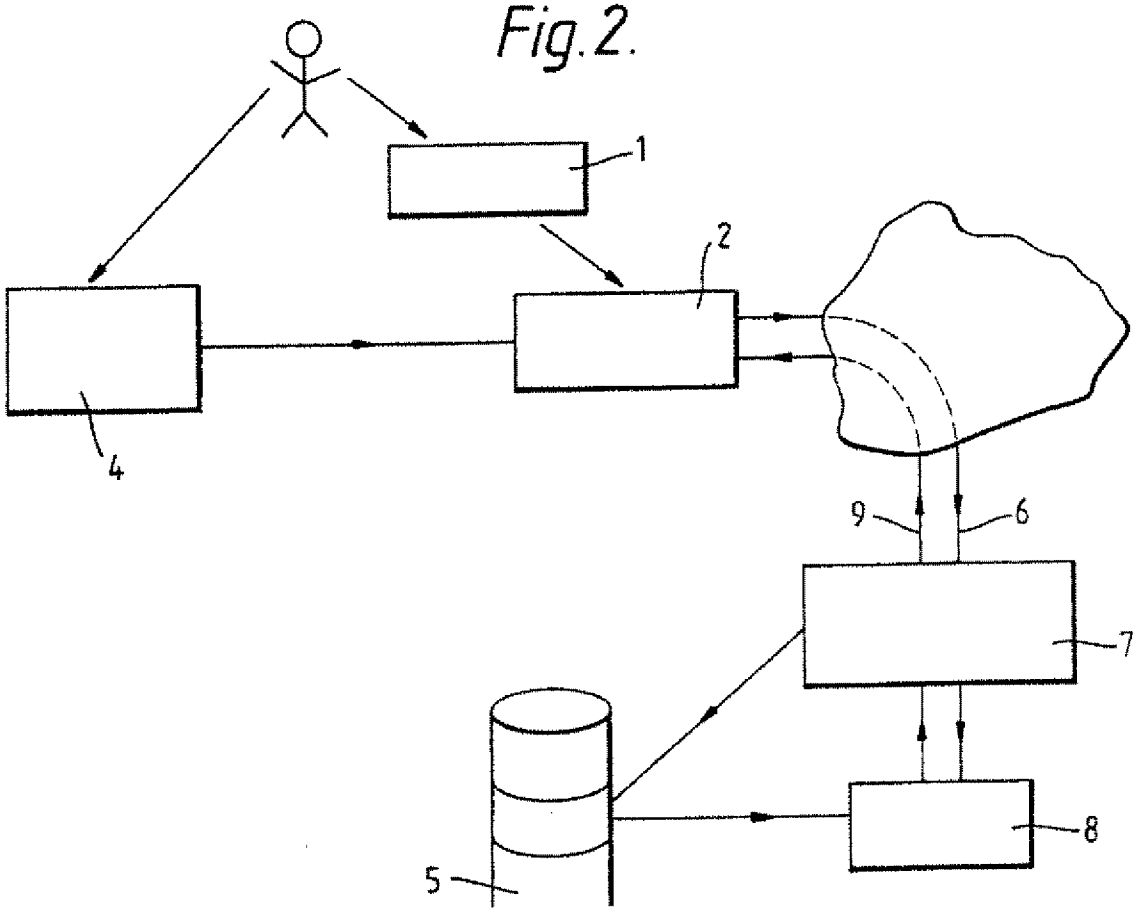


Fig.2.



RECIPROCAL TRANSFER SYSTEM

The invention relates to a transfer of value application in which a user wishes to receive services or goods from a supplier in return for a reciprocal transfer of funds or commitment to recognise the value of the service supplied.

In a typical multilateral decision making situation, each party has a different set of interests and priorities and frequently there has to be a compromise between conflicting decision criteria. For example, in the case of a typical payment situation involving a customer (bank account holder), a retailer and a bank, the customer desires no fraudulent use of the account, the retailer wants guaranteed payment without turning down any customers, and the bank wants no repudiations (particularly successful ones) with processed transactions.

When cash is involved in the transfer of value, the supplier has a guarantee that the funds or commitment supplied by the user will be recognised by the issuer of the cash. However, more recently it has become common for users to tender a credit or debit card which does not in itself guarantee that funds or commitment will be guaranteed by the issuer of the card who provides a main element of the Reciprocal Transfer Service.

The invention is concerned with such multilateral exchanges in which there are at least three parties, that is the user, the supplier, and the reciprocal transfer service which will often be a bank.

In the past, the reciprocal transfer service has had to rely on the decision ability of the supplier to confirm that the user is positively identified and that the supplier is granted authority to access the users account. Generally this has involved requesting the user

to provide his signature which is then visually compared with a reference signature on a card. In some situations, the supplier has been provided with aids to assist with this comparison such as a signature pad.

There is a need for the reciprocal transfer service to have more control over transfers of value and to reduce the reliance on the supplier.

In accordance with one aspect of the present invention, a reciprocal transfer system for use in a transfer of value involving a user who is to receive goods or services from a supplier in return for funds or a commitment to recognise the value of the received goods or services, the system comprising a biometric feature analyser for obtaining from the user at least one biometric feature and for performing a verification analysis on the feature to generate at least one parameter representing the result of the analysis; and control means coupled to the biometric feature analyser for combining in accordance with a predetermined algorithm the verification analysis parameter or parameters with one or more parameters relating to the transfer of value operation and unrelated to the identification of the user, to generate a final risk assessment parameter, the control means being adapted thereafter to indicate to the supplier in accordance with the final risk assessment parameter whether or not the transaction of value can proceed.

In accordance with a second aspect of the present invention, a method of determining whether to perform a transfer of value involving a user who is to receive goods or services from a supplier in return for funds or a commitment to recognise the value of the received goods or services, the user and the supplier conducting the transfer of value in conjunction with a reciprocal transfer system comprises obtaining from the user at

least one biometric feature; performing a verification analysis on the feature and generating at least one parameter representing the result of the analysis; and combining in accordance with a predetermined algorithm the verification analysis parameter or parameters with one or more parameters relating to the transfer of value operation and unrelated to the identification of the user, to generate a final risk assessment parameter, the reciprocal transfer system thereafter indicating to the supplier in accordance with the final risk assessment parameter whether or not the transaction of value can proceed.

We have recognised the inherent problems with biometric methods of user verification which cannot in general give 100% confidence in the verification of identity. Consequently, we now propose combining the results of the biometric verification analysis with other, typically application specific, parameters independent of the biometric features so as to reduce the effect of the uncertainty of the biometric analysis itself.

In one example, the control means has a store for storing at least the recent history of previous uses of the system by each user, that history being used by the control means to constitute one of the additional parameters. Typically, the significance attached to the history will reduce with time and in practice the store may comprise a circular buffer arranged to contain a limited, fixed number of transaction details.

Alternatively, or in addition to the above, the control means may include a store for storing parameters relating to the user which are selected singly or in combination by the control means to constitute one of the additional parameters. These stored parameters relating to the user may include physical characteristics such as

age, sex, social group, psychological profile, handedness, and application related parameters.

In addition or alternatively to the above, the additional parameters may be chosen from the following;

a) Supplier profile parameters eg type of service (for example retailer classification), typical levels of service (for example average transaction values) and risk level of location;

b) Probability of fraud;

c) Value of service;

d) Time and date of transaction;

e) Environmental conditions.

The predetermined algorithm preferably has the form;

$$R = W_1 F_1 (P_1, P_2 \ldots P_N) + W_2 F_2 (P_1, P_2 \ldots P_N) + \ldots$$

where R is the final risk assessment parameter,

W_1 W_2 etc are respective weights,

P_1 P_2 etc are the parameter values, and

F_1, F_2 etc are functions generating a score or absolute value for a given parameter set.

In one application, the control means compares the final risk assessment parameter (R) with at least one threshold to determine whether the transaction of value can proceed.

In the preferred arrangement, the thresholds define 3 bands so that if the final risk assessment parameter falls in one band the control means indicates that the transaction of value can proceed, if it falls in another band the control means indicates that the transfer of value cannot proceed, and if it falls in an intermediate band the control means performs a further algorithm.

This further algorithm may be similar to the algorithm defined above but makes use of different weighting factors so that the parameters are combined in a different manner.

Typically the control means will be sited together with the biometric frature analyser at the point at which the transaction occurs (i.e. point of sale) and off-line to the reciprocal transfer service provider. The control means may also be sited remote from the biometric feature analyser at some central location and on line to the reciprocal transfer service provider. Furthermore there may be a number of biometric analysers connected to a common control means.

This arrangement is particularly suitable for use in an electronic funds transfer at point of sale (EFTPOS) system since the reciprocal transfer system can automatically indicate to the EFTPOS system that a transaction of value can proceed allowing that transfer of value to proceed automatically with a minimum of operator intervention.

The parameter or parameters generated by the biometric feature analyser can indicate the degree to which a submitted biometric feature is simular to a reference feature and preferably these parameters correspond to those described in our co-pending British patent application 89 24848.8 filed on the 3rd November 1989 and entitled "Improvements relating to individual verification" (Agents Ref: 30/3035/01).

An example of an EFTPOS system incorporating a reciprocal transfer system and method according to the invention will now be described with reference to the accompanying drawings, in which:-

Figure 1 is a block diagram of an off-line system; and,

Figure 2 is a block diagram of an on-line system.

In both the reciprocal transfer applications described, a number of parties are involved including at least the following: The consumer's bank, the retailer's bank and the EFTPOS acquirer who gives the service

transfer guarantee to the retailer that the transfer of value may proceed. The EFTPOS acquirer provides apparatus to the retailer to initiate the reciprocal transfer and to assist in the verification of the consumer or user. The consumer's bank issues an identification token such as a card to the consumer to provide a machine readable method of identifying the consumer's account.

In the apparatus shown in Figure 1, a card reader 1 is provided such as a Swipe reader which reads from a consumer's card details of his bank account and the like together with reference biometric data. The account details are fed from the reader to a conventional EFTPOS terminal 2 while the reference biometric data is fed to a microprocessor 3. In this example, the microprocessor 3 is provided locally to the EFTPOS terminal 2. A biometric feature analyser 4 is connected to the microprocessor 3 and is adapted to obtain from the consumer current biometric features. In another example the microprocessor 3 may be a combined element of EFTPOS terminal 2 i.e. one microprocessor may service both the biometric and EFTPOS functions.

In one example, the consumer presents his card to the retailer who places the card in the card reader 1 to allow the reference biometric data and the bank account data to be down loaded to the microprocessor 3 and EFTPOS terminal 2 respectively. The consumer then supplies the necessary biometric data in the form of a submission to the analyser 4. For example, this can comprise writing his signature on a signature pad forming part of the analyser 4, the analyser then obtaining from that signature, data relating to both static and dynamic characteristics of the signature. These features are then supplied to the microprocessor 3 which performs a signature analysis on the submitted data and the

reference data. This analysis would typically be of the form described in more detail in the co-pending British application mentioned above the content of which is included herein by reference. The result of that biometric or signature analysis is the generation of a number of parameters including a confidence of match, a variance, a vulnerability, and a composite biometric level of confidence. The confidence of match parameter is derived from the comparison of the biometric submission with the reference; the variance parameter is derived from an assessment of the level of variance exhibited by the service user or consumer over a period of time and provides an indication of whether the confidence of match parameter is within an acceptable range; and the vulnerability parameter is an assessment of the degree of difficulty in forging/counterfietting the biometric property of the user or consumer. The composite biometric level of confidence is derived from a function which combines the 3 parameters mentioned above together with the possibility of a fraudulent service user. This composite biometric level of confidence parameter is denoted PR_1.

A second parameter PR_2 provides a composite service provider/type of service risk assessment and is generated from one or a combination of the following parameters:

i). Service provider profile. This identifies the service provider and defines characteristics such as type of service (e.g. retailer classification), typical levels of service (e.g. average transaction value) and risk level of location.

The concept of floor limits in point of sale payments is a mechanism used to quantify the risk level of the location, and is not a primary parameter type.

ii). Probability of fraud. This value may vary over time or between service providers. This is an input to

the biometric verification sub-system to allow the composite biometric verification sub-system to allow the composite biometric level of confidence to be generated.

iii). Value of Service. This is the value that is processed by the reciprocal transfer system, e.g. transaction amount.

iv). Time and date. The time of day, day of week, and special seasons of the year may all be significant.

v). Environmental issues. These cover factors such as climatic conditions.

A third parameter PR3 defining a composite user risk assessment is produced for one or a combination of the following parameters:

i). Usage pattern. This is a record of previous use and assumes that significance reduces the further one goes back in time. In practice, this is likely to be a circular buffer limited to a fixed number of transactions.

ii). User profile. This covers any other parameters which are significant to the application such as physical characteristics (e.g. age, sex, social group, psychological profile, handed-ness) and application related parameters.

Each of these parameters PR_1, PR_2, PR_3 is a function of one or more of the base parameters referred to and for example PR_2 can be defined as:

$$\begin{aligned} SCORE = [\ & W_1 * F_{spp} && \text{(service provider profile) +} \\ & W_2 * F_{vts} && \text{(value and type of service) +} \\ & W_3 * F_{td} && \text{(time and date) +} \\ & W_4 * F_{ei} && \text{(environmental issues)]} \end{aligned}$$

where: $W_{1..4}$ are signed weighting values.

F_{ssp} is a function which generates a numeric value by classifying the

details comprising the service provider profile.

F_{vts} is a function which generates a numeric value by classifying the value of the transaction, and possibly also the type of transaction.

F_{td} is a function which generates a numeric value by classifying time, date and possible special periods (e.g. pre-Christmas) into risk levels.

F_{ei} Is a function which tests for special circumstances surrounding environmental issues such as extremes of temperature.

Similarly, Function PR_3 can be defined as:

SCORE = [$W_5 * F_{sup}$ (user profile) +
$W_6 * F_{up}$ (usage pattern, transaction value and type, time and date)]

where:

$W_{5..6}$ are signed weighting values.

F_{sup} is a function which generates a numeric value by classifying the details comprising the user profile.

F_{up} is a function which generates a numeric value by analysing the previous pattern of usage and comparing it to the circumstance surrounding the current one.

The output scores for the three composite parameters are then classified into respective classes or bands to define three such classes, giving the values

X in the range 1 ... x+1 from PR_1

Y in the range 1 ... y+1 from PR_2

Z in the range 1 ... z+1 from PR_3

The microprocessor 3 includes a three dimensional look-up table whose elements are addressed by the band or class values, the three bands derived above being used therefore to address the look-up tables to obtain a risk assessment parameter. Each element of the array contains one of the following set of values:

-1	Pass - proceed with transfer of value
0	Fail - do not proceed with transfer of value
1	Resort to SA_1 for decision
2	Resort to SA_2 for decision
...	...
n	Resort to SA_n for decision

Each SA (Secondary Algorithm) is a function which has as input all the individual parameters listed above plus the composite functions PR_1 - PR_3. For each SA_n, a different set of weights exists, one for each input parameter. Like the above functions, each value is multiplied by the weighting and all products added together to produce a score.

The score of each SA_n is divided into three bands by two thresholds, which are again unique to each SA. Band 1 means fail, band 2 means resort to other procedures, and band 3 means pass.

Clearly, different SA's will attach different priorities to different categories of risk. For example, where the value is modest but the biometric risk is high, more detailed attention will be paid to the biometric

parameters. Similarly, a high value transaction may attach more significance to the usage pattern.

In the Figure 1 example, the card supplied by the consumer contains the biometric reference data as well as the bank account data to enable local operations.

Figure 2 illustrates a different arrangement in which the computer which decides and determines the final risk assessment parameter is located remotely from the EFTPOS terminal 2. In this example, the consumer's card identifies the bank account and the location of the consumer's reference data in a store 5 remote from the terminal 2, typically at the banks premises. Biometric features are obtained from the consumer by the analyser 4 and sent via the EFTPOS terminal 2 along a link 6 to the consumers bank 7. Typically, the link 6 forms part of a conventional EFTPOS system. A computer 8 located at the consumer's bank then extracts the reference biometric data from the store 5 and performs the biometric analysis together with the further risk analysis to generate the final risk assessment parameter in the same way as described above in connection with Figure 1, this final risk assessment parameter then being supplied back to the terminal along a link 9 to control whether the transaction of value proceeds or not.

CLAIMS

1. A reciprocal transfer system for use in a transfer of value involving a user who is to receive goods or services from a supplier in return for funds or a commitment to recognise the value of the received goods or services, the system comprising a biometric feature analyser (4) for obtaining from the user at least one biometric feature and for performing a verification analysis on the feature to generate at least one parameter representing the result of the analysis; and control means (3) connected to the biometric feature analyser for combining in accordance with a predetermined algorithm the verification analysis parameter or parameters with one or more parameters relating to the transfer of value operation and unrelated to the identification of the user, to generate a final risk assessment parameter, the control means thereafter indicating to the supplier in accordance with the final risk assessment parameter whether or not the transaction of value can proceed.

2. A system according to claim 1, wherein the control means include a store for storing a history of previous use by the user, the history being used by the control means as one of the additional parameters.

3. A system according to claim 1 or claim 2, wherein the control means stores parameters relating to the profile of each user for use alone or in combination as an additional parameter.

4. A system according to any of the preceeding claims, wherein one or more of the additional parameters is selected from:

a) Supplier profile parameters;

b) Probability of fraud;

c) Value of service;

d) Time and date of transaction;

e) Environmental conditions.

5. A system according to any of the preceeding claims, wherein the predetermined algorithm has the form:

$$R = W_1 F_1 (P_1, P_2 \ldots P_N) + W_2 F_2 (P_1, P_2 \ldots P_N) + \ldots$$

where R is the final risk assessment parameter,

W_1 W_2 etc are respective weights,

P_1 P_2 etc are the parameter values, and

F_1, F_2 etc are functions generating a score or absolute value for a given parameter set.

6. A system according to any of the preceeding claims, wherein the control means includes comparison means to compare the final risk assessment parameter with at least one threshold.

7. A system according to claim 6, wherein the thresholds define 3 bands so that if the final risk assessment parameter falls in one band the control means indicates that the transfer of value can proceed, if it falls in another band the control means indicates that the transfer of value cannot proceed, and if it falls in an intemediate band the control means performs a further algorithm.

8. A system according to claim 7, wherein if the final risk assessment parameter lies in the intermediate band then the control means determines a further final risk assessment parameter (R') in accordance with the formula:

$$R' = W_1' F_1 (P_1, P_2 \ldots P_N) + W_2' F_2 (P_1, P_2 \ldots P_N) + \ldots$$

where W_1', W_2' etc are respective weights,

P_1, P_2 etc are the parameter values, and

F_1, F_2 etc are functions generating a score or absolute value for a given parameter set.

9. A transfer of value system comprising transaction apparatus for debiting funds from a user and crediting those funds to a supplier; and a reciprocal transfer

system according to any of the preceeding claims, for indicating to the apparatus whether or not the transfer can proceed.

10. A method of determining whether to perform a transfer of value involving a user who is to receive goods or services from a supplier in return for funds or a commitment to recognise the value of the received goods or services, the user and the supplier conducting the transfer of value in conjunction with a reciprocal transfer system, the method comprising obtaining from the user at least one biometric feature; performing a verification analysis on the feature to generate at least one parameter representing the result of the analysis; and combining in accordance with a predetermined algorithm the verification analysis parameter or parameters with one or more parameters relating to the transfer of value operation and unrelated to the identification of the user to generate a final risk assessment parameter, the reciprocal transfer system thereafter indicating to the supplier in accordance with the final risk assessment parameter whether or not the transaction of value can proceed.